Australian Government
Department of Home Affairs

September 2019

Parliamentary Joint Committee on Intelligence and Security

Department of Home Affairs Submission

Inquiry into the Identity-matching Services Bill 2019

Table of Contents

Introduction **3**

Overview of submission 3

Purpose and context of the Bill **3**

Purpose and background 3
Why the face matching services are needed 6
Legislative context 6
Implementation of the FMS 8
Whether the Bill authorises 'mass surveillance' 10
Whether law enforcement agencies should obtain a warrant to use the FIS 11
Whether law enforcement agencies can use the FIS to investigate minor offences 12
Security and data protection 13
Governance arrangements 14
Oversight arrangements 15
Private sector access to the face-matching services 16
Consent 18
Notification 20
Accuracy of facial recognition technology 21
Rule-making powers in the Bill 22

Concluding remarks **23**

Introduction

1. The Department of Home Affairs (the Department) welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Intelligence and Security (the Committee) as part of the Committee's inquiry into the Identity-matching Services Bill 2019 (the Bill).

2. The Bill 2019 helps to implement the Intergovernmental Agreement on Identity Matching Services (IGA) agreed by the Prime Minister and first ministers of the States and Territories at the Council of Australian Governments' Special Meeting on Counter-Terrorism on 5 October 2017.[1]

3. Under this IGA, the Commonwealth and all States and Territories agreed to improve the sharing of information, via new biometric face matching services (FMS), for a range of national security, law enforcement, community safety and related purposes.

Overview of submission

4. This submission provides an overview of the purpose of the Identity-matching Services Bill 2019 and the context within which it has been developed, including the other agreements and policy documents that, together with the Bill, govern the delivery and use of the identity-matching services.

5. The Bill as introduced in Parliament on 31 July 2019 is almost unchanged from the Identity-matching Services Bill 2018 (the 2018 Bill), which was introduced on 7 February 2018.[2] As such, it is in the same form and introduced for the same purpose as the 2018 Bill.

6. This submission discusses issues raised during the hearings conducted by the Committee in 2018 on the 2018 Bill. The 2018 Bill lapsed when the House of Representatives was dissolved on 11 April 2019, and hence the Committee's previous inquiry into the Bill lapsed on that date.

7. This submission also discusses issues that have arisen in relation to the identity-matching services described in the 2019 Bill since the Committee's public hearings on 17 August 2018.

Purpose and context of the Bill

Purpose and background

8. The main purpose of the Bill is to authorise the Department to collect, use and disclose identification information in order to operate the technical systems that support the provision of face matching services.

9. The Bill is made pursuant to the IGA. Under the IGA, the Commonwealth and each of the States and Territories agreed to implement or preserve legislation to implement the face matching services.[3]

---

[1] Available at https://www.coag.gov.au/about-coag/agreements/intergovernmental-agreement-identity-matching-services.
[2] The only amendments in the 2019 Bill compared to the 2018 Bill are changing '2018' to 2019' and changing 'a Australian' in clause 5(1)(i)(i) to 'an Australian'.
[3] IGA, para 8.3

10. The face matching services are set out in the IGA and the Bill. The face matching services provide the ability to use facial images and related identification information to:

    - Verify a person's claimed identity via the Face Verification Service (FVS). The FVS enables a facial image associated with an individual to be compared against a facial image held on a specific government record associated with that same individual to confirm that individual's identity

    - Identify an unknown person or a person holding multiple fraudulent identities via the Face Identification Service (FIS). The FIS enables a facial image to be compared against multiple images held on a database of government records to establish an individual's identity

    - Promote road safety by preventing driver licence fraud and sanction avoidance across jurisdictions (the One Person One Licence Service (OPOLS)). OPOLS enables a facial image to be compared to other images in the National Driver Licence Facial Recognition Solution (NDLFRS) to identify whether a licence holder or applicant holds multiple licences in the same or a different identity across participating jurisdictions.

    - Assist State and Territory road agencies to analyse, de-duplicate and investigate records within their own data holdings (the Facial Recognition Analysis Utility Service (FRAUS)). The FRAUS enables State and Territory road agencies to conduct biometric matching using their own data holdings within the NDLFRS.

11. The Bill also provides for the Identity Data Sharing Service (IDSS). The IDSS will facilitate the transfer of identification information between participating Commonwealth, State or Territory agencies that have a legal basis to share that information. As with all the identity-matching services defined under the Bill, only 'identification information' (as defined at clause 5 of the Bill) will be able to be shared through the IDSS. The purpose for sharing this information must fall within the identity and community protection activities set out in clause 6 of the Bill. Potential uses could be to pass information in support of investigations or to support border processes or service delivery. Unlike the other services described above, there is no matching of images occurring, just transfer of identity information.

12. The Bill itself does not authorise participating agencies to share information through the IDSS (or any of the other identity-matching services). It only provides the Department with specific authorisation to provide the service. All disclosures of information between participating agencies using the IDSS will therefore need to have a legal basis under other legislation, including Commonwealth, State or Territory privacy legislation or agency-specific legislation.

13. The specific types of information that may collected, used or disclosed are specified in the definition of 'identification information' in clause 5 of the Bill. These include:

    - visa and citizenship images held by the Department;

    - passport images held by the Department of Foreign Affairs and Trade; and

    - driver licence images held in a system hosted by the Department on behalf of the States and Territories.

14. These types of information are currently able to be shared with a range of agencies for law enforcement and other purposes, in accordance with relevant legislation including the *Migration Act 1958* (the Migration Act), *Australian Citizenship Act 2007*, *Australian Border Force Act 2015* and the *Privacy Act 1988* (Privacy Act).

15. Driver licence images will be drawn from a new national facial recognition database, known as the NDLFRS which is established by the Bill. The NDLFRS will hold copies of driver licence images that will continue to be held in the local systems of State and Territory road agencies. In addition to supporting the sharing and matching of these images between law enforcement and other agencies, the NDLFRS will also enable road agencies to use the facial recognition technology within the system to analyse their own data using the FRAUS.

16. Some States and Territories have indicated the intent to include images from other document types (for example, proof of age cards or marine licences) within the NDLFRS, without necessarily sharing these with other agencies. This is provided for in the IGA. For this reason the Bill allows for, but does not require, the use of information from these additional document types in the face matching services.

17. The face matching services established by the 2019 Bill will help to strengthen the integrity and security of Australia's identity infrastructure—the identity management systems of government agencies that issue Australia's core identity documents such as driver licences and passports. These systems play an important role in preventing identity crime, which is one of the most common and costly crimes in Australia.

18. The face matching services will also assist with a range of other national security, law enforcement, protective security, community safety, and identity verification activities, including:

    - assisting Australians to verify their identity when accessing government and private sector services
    - the verification of identities of persons of interest in law enforcement investigations
    - the identification of unknown persons of interest in counter-terrorism or law enforcement operations;
    - the protection of government assets
    - the protection of persons with lawfully assumed identities or persons under witness protection
    - improving road safety through the detection and prosecution of traffic offences and the detection of persons with multiple fraudulent driver licences.

19. The Bill, by providing a specific authority for the Department to provide identity-matching services, will form part of a broader legislative framework that governs the use of information by organisations participating in the identity-matching services. This legislative framework and associated independent and parliamentary oversight mechanisms is supported by a range of more detailed legal, policy and other administrative measures, contained in the IGA and other supporting data sharing agreements and policies.

20. The policy and other administrative measures set out in the IGA include:

- The Face Matching Services Participation Agreement (paras 7.2-7.4 of the IGA), which sets out the roles and responsibilities of government participants in the face matching services, including setting out privacy and security requirements.

- The NDLFRS Hosting Agreement (para 7.5), which sets out the roles and responsibilities of the Department and participation road agencies in the management of driver licence information in the NDLFRS.

- The Access Policies, which set out the terms under which participating agencies use the services. This includes the Access Policy for the FVS (para 4.11), the FIS (para 4.23) and OPOLS (para 4.32). There is also a Training Policy (para 9.23) to ensure that staff using the face matching services are properly trained.

Why the face matching services are needed

21. The face matching services facilitated by the Bill will assist in providing a range of service delivery outcomes and help to protect the community from serious crime and terrorism.

22. The FVS will make it easier for a person's image and identity to be safely verified online, making access to government services more secure, accessible and convenient to citizens. In particular, the FVS is to be a key enabler of the government's digital identity program. The digital identity providers which operate as part of this program, including the myGovID service, will need to use the FVS to help verify a person's identity as part of the process of issuing trusted digital identity credentials that will be used to access online services.

23. The FVS will help to protect Australians from identity crime, which continues to be one of the most common crimes in Australia. One in four Australians will be a victim of identity crime at some point in their lives, with an estimated annual cost of more than $2 billion to the economy.

24. The new face matching services enabled by the Bill will also make it harder for people to fraudulently obtain identity documents in an attempt to conceal their true identity.

25. The FIS will also greatly assist our law enforcement and national security agencies to combat criminal and security threats, by providing a means to quickly match facial images drawn from existing databases in order to identify unknown persons of interest.

Legislative context

26. The 2019 Bill is not intended to govern the full operation and use of the face matching services. The Bill has been developed to provide a specific legal basis for the Department's role as the operator of the technical systems that facilitate the services, and to place appropriate safeguards around the operation of those systems and the scope of the identity-matching services that they provide.

27. In doing so, the 2019 Bill will become one part of a larger network of legislation that governs information-sharing between organisations participating in the identity-matching services. This includes the Privacy Act, State and Territory privacy legislation, and other legislation governing the specific functions and operations of agencies participating in the identity-matching services as providers or users of data.

28. The 2019 Bill does not seek to amend or replace any existing legislation, or to provide a broad exemption to privacy legislation for organisations participating in the identity-matching services. Agencies that make available data through the services, and organisations seeking to access data through the services, will continue to be subject to the legislative privacy protections and information-sharing restrictions that apply to them. Agencies will need to have regard to their applicable legislative authorisations when participating in the services, including in relation to the organisations with which they can share information and the purposes for which they can do so.

29. However, clause 19 of the Bill does authorise the disclosure of State and Territory driver licence information to the NDLFRS on the basis of general State and Territory laws that authorise disclosure under a Commonwealth law. However, it is the intention of the Department to rely on specific State and Territory legislation authorising disclosure of driver licence data (such as the laws referred to below).

30. The 2019 Bill seeks to enable, rather than to authorise, the use of the services by various government agencies and (in more limited cases) private sector organisations, which must have a basis to collect, use and disclose personal information under other legislation.

31. In some cases new or amended legislation will need to be introduced to authorise or provide specific legal basis for an agency's or organisation's participation in the identity-matching services.

32. For example, the Australian Passports Amendment (Identity-matching Services) Bill 2019 will provide a specific legislative basis for the Department of Foreign Affairs and Trade to make available passport information on an automated basis to support the identity-matching services.

33. In addition, the States and Territories agreed under the IGA to introduce or preserve legislation to facilitate their participation in the identity-matching services, including the provision of driver licence images via the face matching services. As at August 2019, five States and Territories have such legislation in place. This includes two jurisdictions, New South Wales and Queensland, which have passed legislation since the 2018 Bill was introduced in February 2018.

34. The State and Territory legislation consists of the following:

- New South Wales. The *Road Transport Amendment (National Facial Biometric Matching Capability) Act 2018* (NSW) amended the *Road Traffic Act 2013* (in November 2018). This legislation provides for the release of photographs and associated personal information to, and the collection of that information from, the interoperability hub and NDLFRS established under the 2019 by an authorised NSW government agency.

- Victoria. *Road Safety Act 1986* (Vic). This legislation authorises sharing of driver licence information pursuant to a relevant intergovernmental agreement (in this case, the IGA).

- Queensland. Amendments made to the *Transport Planning and Coordination Act 1994* (Qld) (and other Queensland legislation) made by the *Police and Other Legislation (Identity and Biometric Capability) Amendment Act 2018* (Qld) (April 2018). This legislation authorises the disclosure of Queensland driver licence information to the Department.

- South Australia. *Public Sector (Data Sharing) Act 2016* (SA). This legislation authorises the disclosure of South Australia information to the Department under an agreement pursuant to the South Australian legislation.

- Tasmania. Amendments to the *Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010* (Tas) made by the *Vehicle and Traffic (Driver Licensing and Vehicle Registration) Amendment (Identity Matching Services) Regulations 2017* (Tas) (December 2017). These regulations are made under the *Vehicle and Traffic Act 1999* (Tas). This legislation authorises the disclosure of Tasmania driver licence information to the Department.

35. Western Australia, the Northern Territory and the Australian Capital Territory have not yet passed legislation to support their provision of driver licence images via the face matching services under the IGA.

36. The 2019 Bill is designed to further strengthen the legal basis for the Department to collect, use and disclose personal information for purposes associated with providing the NDLFRS and the identity matching services. The Bill is also designed to control and limit the purposes for which the Department may collect, use and disclose personal information for purposes related to the NDLFRS and the identity matching services.

37. The Department will be required to meet the obligations under the Australian Privacy Principles (APPs) in the Privacy Act, and other specific legislation. In this context, it should be noted that the APPs permit Commonwealth government agencies (including the Department) to collect personal information where it is reasonably necessary for, or directly related to, the agency's functions. In addition, the APPs permit Commonwealth agencies to collect sensitive information (such as facial biometric information) under the authority of an Australian law, which can include a Commonwealth, State or Territory law.

38. Further information about how privacy legislation will apply generally in relation to the services is available in the Department's response to the Committee's question on notice IMS/011, made by the Committee on 17 August 2018 (available in the Department's submission 12.3 to the 2018 inquiry).

Implementation of the FMS

39. The technical systems that support the identity-matching services and which fall within the scope of the Bill are:

    a. the interoperability hub, which supports the services by acting as a router to transmit requests for a face-matching service, and responses to those matching requests, between participating agencies; and

    b. the NDLFRS, which will comprise a federated database of State and Territory licence information hosted by the Department on behalf of the States and Territories, with an in-built facial recognition system to conduct face-matching against the database.

40. As the operator of these systems, the Department will not have access to the identification information contained in matching requests or responses that are routed through the interoperability hub, or to the facial images or other identification information stored in the NDLFRS. The Department will only be able to use the identity matching services, or obtain

access to information by using those services, on the same basis as other participating agencies, or for technical or troubleshooting purposes. The Department will retain and have access to certain transaction data about matching requests and responses that is necessary for auditing and oversight purposes but this will not contain any personal or sensitive information about an individual.

41. As set out in the explanatory memorandum, the Bill contains a range of privacy protections for the information handled by the Department in the course of developing and operating these systems. These include annual reporting on the provision of the services (clause 28), an offence for unauthorised disclosure of identification information by persons working on behalf of the Department (clause 21), and a statutory review that will be tabled before both Houses of Parliament (clause 29).

42. The Department has also adopted a 'privacy by design' approach to the development of the NDLFRS and the identity-matching services, in accordance with the guiding policies listed in para 2.1 of the IGA. Accordingly, Privacy Impact Assessments (PIAs) have been conducted throughout the design phases of the FMS. For example, the technical systems that support the face matching services, in particular the interoperability hub and NDLFRS, have been independently reviewed and assessed for privacy impacts, with the outcomes consistent with the APPs and no significant compliance risks identified.

43. To date the Department has commissioned PIAs on:

    - the technical design of the FMS Interoperability Hub
    - the technical design of the NDLFRS
    - the use of the FVS by the Department of Foreign Affairs and Trade (DFAT) and Australian Federal Police (AFP) to access visa and citizenship information
    - the use (or potential use) of the FMS by the law enforcement, anti-corruption and security agencies listed in clause 8(2) of the Bill.

44. Additional PIAs have also been commissioned by other agencies on:

    - the participation of state and territory road agencies in the FMS; and
    - the use of the FVS by the Australian Taxation Office (ATO), in the context of the myGovID digital identity service.

45. The Department is continuing to build the NDLFRS, as agreed by all jurisdictions under the IGA. This includes collection of relevant state and territory driver licence information, including images, by the Department. This is expected to occur on an ongoing basis up to 2021.

46. The collection of state and territory drivers licence information by the Department is permitted by relevant APPs under the Privacy Act. Relevantly, the APPs:

    - permit the Department to collect personal information (such as names and dates of births) where it is reasonably necessary or directly related to the Department's functions or activities (under APP 3). These functions and activities include being responsible for implementation of the NDFLRS and the identity-matching services pursuant to the IGA.

- permit the Department to collect sensitive information (as a facial biometric information) where it is authorised under an Australian law, which can include a State law (the list of relevant State laws appears above) (under APP 3.4(a)).

- permit the Department to use or disclose personal information (including sensitive information) where that use or disclosure: is for the same purpose as which the information was collected, is authorised under an Australian law, or is for law enforcement related purposes (APP 6) .

47. The collection of information in the NDLFRS is required to allow necessary technical work to be done to establish the system. However, any operational use of the face matching services using this information will be entirely at the discretion of the State or Territory agency that supplied this data.

Whether the Bill authorises 'mass surveillance'

48. It has been argued in submissions to the 2018 Inquiry that the Bill might authorise 'mass surveillance', 'real-time monitoring' or 'live facial recognition' of persons in public places.

49. The FIS enables police, anti-corruption and security agencies to identify an unidentified person using a facial image of that person. The specific list of agencies authorised to use the FIS is set out in subclause 8(2) of the Bill.

50. It does not facilitate 'mass surveillance' or live facial recognition because:

- The technical systems supporting the FIS are designed so that a human operator must submit an image for each FIS request individually (this creates the audit trail) and resolve the match responses provided. The system does not allow for automated submissions of images or a live feed of video images or for decision without human intervention.

- The FIS can only be used to identify a particular person in the course of one of the activities set out in subclauses 6(2)-(6) of the Bill (activities relating to preventing identity fraud, law enforcement, national security, protective security or community safety). The Bill does not authorise the use of the FIS to identify a person merely because they are in a particular location.

- Governance and policy arrangements established under the IGA such as the Face Matching Services Participation Agreement impose strict requirements for use of the FIS, which prohibit indiscriminate use of the service.

51. However, it should be noted that it is possible for an agency to use a still image of a person extracted as a single still image from CCTV. The still image could be individually used to attempt to ascertain that person's identity using the FMS. However, it is not technically possible to 'live stream' footage from a CCTV camera into the FIS. The use of any images extracted from CCTV would be governed by other protections in the Bill.

52. The Bill will enable the Department to provide agencies with the tools to quickly and securely share and match data that they can lawfully collect, use and disclose to other agencies. Participating agencies need to have their own legal basis to collect information that they wish to use in a query or receive in response to a query, and to share it in the course of one or more of the identity and community protection activities, before they can use the services.

53. Mass or indiscriminate use of the face-matching services would not be feasible in practice, given that the systems supporting the services are not designed to support this type of usage and that agencies would not have the resources, including personnel sufficiently trained in facial recognition, to devote to this kind of usage.

54. Only a specified list of law enforcement, anti-corruption and security agencies may use the FIS. It is therefore not possible for private sector organisations (such as operators of stadiums) or local government authorities to use the FIS to scan a crowd to identify persons.

Whether law enforcement agencies should obtain a warrant to use the FIS

55. It has been suggested in submissions to the Committee's 2018 inquiry on the Bill that law enforcement agencies should require a warrant to use the FIS.

56. The Department recognises that the privacy implications associated with the FIS are greater than those of the other identity-matching services as it provides for the identification of unknown persons as opposed to validating the identity of known persons. This is why the FIS is subject to greater protection under the Bill, including the limitation of access to identified agencies (listed in subclause 8(2)) and the restriction of some of those agencies to limited purposes (see for example, paragraph 8(2)(a)). The supporting agreements between the Department and participating agencies, as well as standard operating policies will support these outcomes.

57. The Department does not consider that a warrant requirement for access to the FIS is justified.

58. The Bill is designed to facilitate access to the FIS for specified identity and community protection activities, by specified agencies that have a lawful basis to do so under other legislation. In addition, the governance arrangements for access to the services, particularly the FIS will have strict controls to ensure access is lawful and proportionate.

59. One of the purposes of the FIS is to assist law enforcement and national security agencies to identify persons of interest in their investigations and other activities by providing them with better tools to share and match information than those currently available to them. One of the key benefits of this will be the increased speed with which these agencies can determine the identity of a person of interest, and take any steps necessary to protect the community from harm.

60. As some of the identity and community protection activities specified in the Bill can be very time-sensitive, such as activities in relation to national security (subclause 6(4), missing persons (subparagraph 6(6)(a)(i)) and risks to public safety (paragraph 6(6)(b)), it is likely that a requirement to obtain a warrant would significantly impede the ability of government agencies to use the FIS to carry out their legislated functions.

61. Obtaining a warrant is a resource intensive process, both for the applicant agency and for the issuing authority hearing the application. The time involved in preparing, reviewing and granting a warrant application to use services would:

    - significantly delay, and in some circumstances undermine, law enforcement and national security investigations

- impede operational activity, including the prevention of criminal acts
- divert resources from investigations, and
- cause delays in circumstances where risks to personal and public health and safety are extant.

62. The Attorney-General's Department's (AGD) *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers of 2011* (the Commonwealth Offences Guide) describes the circumstances when it would be appropriate to require agencies to obtain a warrant. The circumstances under the Commonwealth Offences Guide are:

- Where there is entry to premises without consent
- Where it is required to use reasonable force against things or persons in the execution of a warrant
- Where there is seizure of items, and
- Where there is a monitoring regime involving the above matters.

63. Some Commonwealth legislation also requires a relevant government agency to obtain a warrant in some circumstances in the investigation of offences. One example is the requirement under the *Telecommunications (Interception and Access) Act 1979* for certain agencies to obtain a warrant to intercept live communications, such as a person's telephone conversations, or obtain a warrant to access stored communications such as emails. Another example is the requirement under the *Surveillance Devices Act 2004* for certain agencies to obtain a warrant to use a surveillance device in various circumstances, such as on specified premises. Warrants are required in these circumstances due to the level of privacy intrusion associated with intercepting and accessing live communications, accessing stored communications and using surveillance devices.

64. This level of privacy intrusion does not apply in relation to use of the FIS. In using the FIS, the agency will submit a probe image of a person that has already been obtained by that agency under current legislative frameworks. Use of the FIS does not involve entry into private premises, use of force, the seizure of items, the obtaining of private communications or the surveillance of a person. The Bill facilitates the sharing of information between agencies, but relies on agencies having a separate legal authority for that information-sharing. Police already share this information subject to existing legal frameworks.

65. Overall, the Department considers that the privacy safeguards built into the Bill, as well as those contained in the administrative and policy arrangements supporting the services, are sufficient to ensure that the services are only used in appropriate circumstances and by appropriate authorities.

Whether law enforcement agencies can use the FIS to investigate minor offences

66. It was argued in submissions to the Committee's 2018 inquiry on the Bill that law enforcement agencies may be able to use the FIS for minor offences.

67. The IGA (at para 4.21(b)) and supporting policy and data sharing agreements with the States and Territories largely limit use of the FIS, when used for general law enforcement purposes, to offences with penalties of not less than three years imprisonment.

68. The Bill itself does not include this restriction, but access to the FIS under policy and data sharing arrangements will capture this limitation subject to some flexibility to accommodate variations in penalties for some offences (e.g. common assault) across different States and Territories. This reflects para 4.22 of the IGA, which contemplates use of the FIS in these circumstances where a State or Territory is using only its own data.

69. More broadly, the annual reporting arrangements under the Bill require an agency to identify the kind of identity and community protection activity for which each request for the FIS is submitted (see subparagraph 28(1)(a)(v) of the Bill). In effect, this means that an agency must record the reason for using the FIS for each request. This will create an audit trail, so that agencies will need to be able to justify each use they make of the service. Under policy and data sharing arrangements, the Department will have the ability to query or suspend an agency's access to the FIS in the event the agency is using the service inappropriately.

70. In addition, the annual reporting provisions in the Bill will require public reporting on the number of times that agencies use the FIS for law enforcement. If an agency uses the FIS more frequently than is justifiable, this would become subject to public scrutiny in the annual report.

Security and data protection

71. The development and operation of the NDLFRS and the interoperability hub by the Department will adopt best practice security and access arrangements.

72. The systems will comply with the requirements of:

- the Australian Government Protective Security Framework, which provides guidelines and minimum standards in relation to protective security for Australian Government agencies and officers, and

- the Australian Government Information Security Manual, which sets out the standards that govern the security of government ICT systems.

73. The systems will also be subjected to independent penetration and vulnerability tests, and an independent security review as part of the Information Security Registered Assessors Program (IRAP) certification process, which is the best-practice Commonwealth information security assessment. The Australian Signals Directorate (ASD) is being consulted as part of this process.

74. Access to the identity-matching services will be restricted to individuals that have been authorised by the participating agencies. Users will only be provided with access to the specific functions they have been authorised to perform. Most users will only be given access to the FVS function, and access to the FIS will be much more limited.

75. Protection of information at participating agency-level will rely on existing data security controls that those agencies already apply when handling personal information. Within the framework of the Participation Agreement, data-holding agencies will be able to stipulate any additional

measures that they require to support the secure exchange of images. Regular audits will help ensure that these protections are functioning appropriately.

76. Management of data breaches is governed by the data breach notification provisions in Part IIIC of the Privacy Act. These provisions will apply to the information held by the Department in the NDLFRS or in the operation of the identity matching services.

Governance arrangements

77. The legislative framework governing the use of the services provides a range of protections for the information that will be shared through the services. These legislative protections are just one aspect of the privacy safeguards surrounding the services. The administrative and policy arrangements that the Department is putting in place to support its provision of the services, also contain further protections.

78. Administrative and policy arrangements to be established by the Department include additional privacy protections that participating agencies need to comply with before obtaining access to the services. These requirements, set out in clause 9.9 of the IGA, will be to:

    a. provide a statement of the legislative authority or basis on which the entity may obtain identity information through the face-matching services,

    b. be subject to a privacy impact assessment which includes consideration of the entity's use of the face-matching services (except where the entity's use is expressly exempt from relevant Commonwealth, State or Territory privacy legislation),

    c. enter into arrangements for the sharing of identity information with each data-holding agency it wishes to receive information from,

    d. provide appropriate training to personnel involved in the use of face-matching services, and

    e. conducting annual compliance audits in relation to the use of face-matching services.

79. These requirements will be set out in a common Participation Agreement between all participating Commonwealth, State and Territory agencies in order to provide a legally binding framework within which agencies will negotiate details of data sharing arrangements, so that these arrangements meet minimum privacy and security safeguards in order to support information sharing across jurisdictions.

80. These arrangements are being established and agreed between the Commonwealth and all States and Territories. They are based on the principle that each State and Territory retains control over decisions on how its data is shared.

81. Pursuant to the IGA, the Department will conduct reviews at different points to provide mechanisms to ensure that the identity-matching services are being implemented and continue to operate as intended. Changes to this framework that may arise from these reviews will require broad national agreement, providing an additional level of control over any future expansion of the scope of the face-matching services.

82. Some submissions to the Committee's 2018 inquiry into the Bill argued that too many of the core principles, governance arrangements and oversight mechanism for the identity-matching services are contained in supporting documentation such as agreements and policy documents, and that more of this material should be in the Bill.

83. However, as stated above the Bill is not intended to govern the full operation and use of the identity-matching services. The services are subject to existing legislation applying to users of the services, including privacy legislation and legislation governing the agencies themselves. The Bill provides a legal basis for the Department's operation of the NDLFRS and the identity-matching services.

84. The identity-matching services involve access to both Commonwealth and State and Territory data sources. The IGA sets out, in detail, the agreement between the jurisdictions on a range of matters related to the services, including guiding principles, governance and oversight mechanisms.

85. The IGA also provides for certain matters to be managed by agreements made between the parties. This includes, for example, the Participation Agreement, which will set out terms and conditions, including minimum privacy and security safeguards, for all agencies participating in the services, and the NDLFRS Hosting Agreement, which sets out arrangements for the Department's hosting of State and Territory data in the NDLFRS. The matters dealt with in these agreements are subject to negotiation and agreement between Commonwealth, State and Territory participants. It may not be appropriate to fix this level of detail in legislation.

Oversight arrangements

86. The key oversight mechanisms contained in the Bill are:

- Public annual reporting on use of the identity-matching services (clause 28)
- A statutory review of the identity-matching services commencing within five years (clause 29)
- Consultation with the Information Commissioner and the Human Rights Commissioner in the making of certain rules by the Minister (clauses 5(4)(b), 7(5)).

87. The Bill (clause 28) requires the Minister to report to Parliament annually on the operation of the services. This is an important transparency measure which will assist the Parliament with its oversight of the operation of the identity-matching services.

88. It was argued in submissions to the Committee's 2018 inquiry that the Bill should include further information in the annual report, such as information about data breaches, security incidents and unauthorised usage or disclosure.

89. The annual reporting provisions in the Bill largely require the provision of statistical information on the use of the identity-matching services. This is intended to provide similar types of public information as are required in the annual reports under the *Surveillance Devices Act 2004* and the *Telecommunications (Interception and Access) Act 1979*.

90. Management of data breaches is governed by the data breach notification provisions in Part IIIC of the Privacy Act. These provisions will apply to the information held or processed in the NDLFRS and through the identity-matching services. It is not necessary to duplicate data breach reporting by requiring this information to be included in the annual report under the Bill.

91. In relation to other matters, such as security incidents and unauthorised use or disclosure, reporting on these issues may not always be appropriate, for example if it would disclose information about the security architecture of the systems. In addition, the Department may not have information about all instances of unauthorised use or disclosure if these occur at participating agency level. However, this information will be able to be captured, and properly investigated and assessed, through annual audit requirements on participating agencies using the services, and the various reviews of the services required under the IGA (every three years) and the Bill (clause 29). These mechanisms provide a more appropriate opportunity to consider these issues in detail and identify options to address them.

92. The Bill (clause 29) requires the Minister to cause a statutory review of the Bill to be commenced within five years of commencement of the Bill. It was argued in submissions to the Committee's 2018 inquiry that the period of time for the statutory review should be reduced. However, the implementation of the face-matching services across all jurisdictions will be incremental over the next few years. A period of up to five years for the statutory review to commence is appropriate to ensure that adequate information is available from each of the jurisdictions to ensure the review is thorough and comprehensive.

93. In addition, the statutory review period of five years is less than that contained in some other Commonwealth legislation providing for statutory reviews. For example, section 251 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* provided for a review to be conducted within seven years.

94. It has also been argued in submissions to the Committee's 2018 inquiry that a biometrics commissioner or equivalent office should be established. Whilst the decision about whether to establish such an office would be a matter for government, the Department notes that the role of the UK Office of the Biometrics Commissioner primarily relates to review the retention and use by the police of DNA samples, profiles and fingerprints, and police use of facial biometrics.

95. The Bill is not seeking to expand the circumstances in which police can collect biometric information from individuals, or govern their use or retention of biometric information. The Bill will enable the Department to facilitate information-sharing between agencies that already have a legal basis to do so. The extent to which existing or new police powers in relation to biometric information require greater oversight is a separate issue, outside the scope of the Bill.

96. In addition, agencies participating in the identity matching services will continue to be subject to existing oversight arrangements that apply to their activities or functions. At the Commonwealth level, this includes, the Inspector-General of Intelligence and Security (for intelligence agencies), the Office of the Australian Information Commissioner, and the Commonwealth Ombudsman. Comparable oversight bodies also operate at the State and Territory level.

97. In relation to auditing, the Department has entered into a Memorandum of Understanding (MOU) with the Office of the Australian Information Commissioner (OAIC) to conduct annual audits in relation to use of the face matching services. The Department has funded the OAIC to undertake these audits.

Private sector access to the face-matching services

98. Private sector organisations conduct a range of identity verification activities on a daily basis and are a key partner in combatting identity crime and other criminal activity such as money laundering and the financing of terrorism.

99. Expanding use of the Document Verification Service (DVS) is making it harder for criminals to use fictitious identities, but is creating incentives for them to use documents in stolen identities. Providing the private sector with access to the FVS will help prevent this from occurring, protecting the identities of innocent Australians and helping companies such as financial institutions and telecommunications providers to better meet their regulatory customer identification obligations that help to contribute to national security and law enforcement outcomes.

100. Private sector access to the FVS would be on similar terms to the DVS, notably that they must obtain the consent of individuals before seeking to match images through the service. Governance of the DVS involves robust contractual arrangements and a comprehensive program of independent audits of users of the services, which has resulted in suspension of access to the service for some entities for non-compliance with DVS terms and conditions.

101. With this in mind, private sector usage of the face matching services is envisaged under clause 5.3 of the IGA. Private sector access to the FVS will be subject to certain conditions expressed in clause 5.4 of the IGA. In order to fully implement the IGA, the Bill facilitates future use of the face-matching services by the private sector.

102. Clauses 7(2)-(4) and clause 10(2) of the Bill apply a range of privacy safeguards to private sector usage of the face matching services. These include:

- the private sector will only have access to verification services
- verification of a person's identity must be reasonably necessary for the functions of the organisation
- the organisation must have a legal basis to use the service
- the organisation must have the consent of the person whose identity is being checked
- the organisation must be subject to the Privacy Act
- the organisation must carry on activities in Australia or reside in Australia, and
- private sector usage of the services will be reported on in the annual report to be tabled in Parliament.

103. Subject to the passage of the Bill, the nature of private sector access remains a matter for Ministers at the Commonwealth and State and Territory level to determine, guided by the IGA.

104. Under clause 5.4 of the IGA, access to State or Territory data for private sector users will also be subject to further safeguards, including:

- the written agreement of the relevant State or Territory minister
- a privacy impact assessment covering the particular type of organisation seeking access
- compliance with the Commercial Service Access Policy, and
- an audit and compliance program.

105. In addition, private sector users will only get a 'match / no match' response, with no provision of further biographic or facial image information.

106. These safeguards will ensure that private sector access to the face-matching services is appropriately limited and proportionate to their need to verify identity in the provision of services.

107. Nothing in the Bill mandates the use of the FVS by private sector organisations. Any use of the FVS by the private sector will be on an opt-in basis, and user organisations will need to ensure that they meet their obligations under the Privacy Act, and other legislation that applies to them, including to obtain consent from their customers in relation to the use of their identification information in an FVS check. This may mean, for example, providing alternative options for identity verification using the DVS or other identity verification processes if a customer does not consent to the use of their identification information through the FVS. As is currently the case for the private sector's use of DVS, the Department's future audit activities would focus on ensuring that consent was properly obtained for use of the FVS.

Consent

108. Submissions to the Committee's 2018 inquiry on the Bill raised concerns in relation to how a person may give consent to the use of their personal information in the provision of an identity-matching service.

Genuine consent

109. The first consent-related issue relates to how a person can genuinely consent to the use of their identification information in the services.

110. In summary, it was argued that a person may not be able to give genuine consent to their identification information being used to verify their identity using an identity-matching service. It is argued that a person who requires an important or essential service, such as the provision of a bank account, may not have a genuine choice to decline to have their identity verified through a face-matching service. This issue is raised particularly in relation to the FVS.

111. Under the Bill, both government agencies and private sector organisations may potentially use the FVS. Under clause 10(2) of the Bill, any entity that wishes to use the FVS must have a legal basis to collect, use or disclose identification information. For Commonwealth, State and Territory government users of the FVS, consent is only one of a number of legal bases that agencies may rely on to use the FVS. For private sector and local government users of the FVS, paragraph 7(3)(b) of the Bill provides that consent of the individual whose identity is being verified is required in all cases.

112. The concept of 'consent' in the Bill is based on relevant provisions of the Australian Privacy Principles (APPs) in the Privacy Act. APP 3.3(a) permits an APP entity to lawfully collect sensitive information about an individual with that person's consent and where it is reasonably necessary for, or directly related to, the entity's functions or activities. In addition APP 6.1(a) permits an APP entity to lawfully use or disclose personal information about an individual for a secondary purpose with that person's consent.

113. The Office of the Australian Information Commissioner's *Australian Privacy Principles Guidelines* (APP Guidelines) set out the requirements for 'consent' as follows:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

114. The obtaining of consent for use of the FVS will operate in the same way as it does in the context of the existing DVS.

115. The DVS relies on its private sector users meeting the consent and other privacy requirements referred to in the APP Guidelines. There are regular audits to ensure users are meeting their obligations in relation to their use of the services, including consent requirements. The Department will also publish information about the services on a website, similar to that contained on the DVS website, to help individuals understand how their information is collected and used through the services.

116. Under the IGA (para 5.4), private sector access to the FVS to match against State and Territory data would also be subject to the outcomes of privacy impact assessments on each type of organisation that will use the services, and an FVS Commercial Service Access Policy including an audit and compliance programme. These processes will consider processes for obtaining consent, and provide an opportunity to identify any non-compliance with consent obligations.

Consent for secondary usage and notification

117. The second consent-related issue raised in relation to the Bill concerns whether persons who have consented to use of their identification information for the provision of an identity document (such as a driver licence or passport), have also consented to the secondary use of their identification information in the identity-matching services.

118. The use and disclosure of personal information for secondary purposes without the consent of an individual is clearly contemplated in certain circumstances under the APPs and comparable State and Territory privacy legislation.

119. APP 6 in the Privacy Act permits the use or disclosure of personal information for secondary purposes without consent in certain circumstances. These include where the disclosure is: authorised or required under an Australian law or court/tribunal order (APP 6.2(b)); or for enforcement related activities conducted by or on behalf of an enforcement body (APP 6.2(e)).

120. In its role facilitating the identity-matching services, as the operator of the interoperability hub and the NDLFRS, the Department does not interact directly with individuals whose information is used in the services. These interactions are conducted by the agencies which seek to use the services and/or the data-holding agencies which make their information available via the services. Therefore it is impracticable for the Department to collect consent directly from individuals for the secondary use of their information in the identity-matching services.

121. Instead, the Department will rely in part on APP 6.2(b), which permits use or disclosure where authorised by a Commonwealth, State or Territory law – in this the case, the Bill if

passed. This will enable the Department to lawfully fulfil its role in transmitting information between agencies participating in the identity-matching services.

122. Under the IGA, all information-sharing through the services will also be subject to the separate legal basis that each participating agency has to collect, use and disclose identification information, and any legislative restrictions that apply to those activities including under the Privacy Act or other applicable privacy legislation. This means that data-holding agencies who collect information for one purpose (such as road agencies collecting information in order to issue driver licences), must also have a legal basis to share that information through the identity-matching services, whether based on consent or another legislative authority.

123. In most cases, data-holding agencies already have legislative authority to share identification information without the consent of the individual for some or all of the activities for which the identity-matching services will be available. For example, information-sharing for law enforcement purposes already occurs under a range of legislation.

124. It would be impractical for data-holding agencies to allow persons to opt-out of having their identification information available to the NDLFRS and the identity matching services. To do so would effectively provide criminals with the ability to 'opt-out' of their information being made available to law enforcement agencies that are investigating criminal offences, or allow people using fraudulent identity documents to avoid detection. This would defeat the main purposes of the legislation.

125. In addition to legislative protections that apply to all agencies participating in the services, the Department will make publicly available information on the operation of the identity-matching services so that the community is aware of and can understand how their information is used through these services.

Notification

126. Another important issue is the extent to which individuals are notified, or made aware, of the collection of their information in the NDLFRS or the identity matching services.

127. Very broadly, APP 5 contains a general requirement for APP entities (including the Department) to take reasonable steps to notify individuals, or make them aware, about the collection of their personal information and how that information is used. This requirement will apply to the Department in its operation of the NDLFRS and the provision of identity-matching services facilitated through the interoperability hub.

128. Pursuant to APP 5, the Department will take reasonable steps to make people aware of the different notice requirements in APP 5 such as the fact that their facial images and identification information may be used in the identity matching services, including the FIS.

129. It is not practical for the Department to notify individuals directly that their information is being collected in the NDLFRS. This is because the Department is not collecting information directly from individuals in its role as operator of the interoperability hub and NDLFRS. However, the Department will take other steps to make individuals aware of the relevant APP 5 notice requirements. For instance, notification to individuals will rely to a significant extent on data-holding agencies, including State and Territory road agencies, to inform individuals about the intended use of their information in the identity-matching services. The Department will

work closely with these agencies to ensure that these notifications are updated as the services come online for different data sources.

130. The Department will also make publicly available information on the operation of the identity-matching services and the NDLFRS so that the community can understand how their information is used through these services.

131. A further point is that APP 5 does not require agencies to notify persons when their information is accessed (rather than collected). Accordingly, individuals will not be specifically notified when their image is accessed through FIS. This is similar to current law enforcement and security agency practices, where identification information may be obtained by these agencies from other agencies for the purpose of investigations. These agencies currently would not typically notify these individuals that their information had been obtained in the course of an investigation. Notification in these circumstances would warn a person that they were under investigation and give them the opportunity to flee, destroy evidence or compromise witnesses.

Accuracy of facial recognition technology

132. Facial recognition systems involve a combination of automated matching, with results subject to human review, particularly where agencies seek to identify an unknown person. This is certainly the case for the FIS. As such, the accuracy of facial recognition systems should not be assessed on the performance of biometric matching algorithms alone.

133. The Department also notes that the accuracy of facial recognition technology continues to improve over time. For example, according to testing by the US National Institute of Standards and Technology (NIST), the accuracy of facial recognition algorithms improved by 20 times between 2014 and 2018. After testing 127 algorithms from 39 leading developers, the combined failure rate was 0.2 percent. This means that systems were 99.8 percent accurate compared to 96 percent in 2014.[4]

134. Based on testing by NIST, the algorithms used by the Department and the Department of Foreign Affairs and Trade in operating the face matching services are amongst the most accurate commercially available algorithms in the world.

135. The Department conducts ongoing testing and tuning of the facial recognition software or algorithms used to support the face matching services, using Australian datasets, to continually improve the accuracy of systems supporting these services. This testing is conducted in controlled conditions designed to simulate actual use cases.

136. Matching results that seek to identify an unknown person will be reviewed by trained facial recognition experts to protect against the possibility of false matches. In other words, decisions that serve to identify a person will never be made by the technology alone.

[4] P. Grother et al, *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, National Institute of Standards and Technology, NISTIR 8238, November 2018, pp. 2, 36, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

137. Research published by the Proceedings of the National Academy of Sciences in the United States indicates that the most accurate biometric matching performance is achieved by using a combination of algorithms and human operators with specialist training in facial recognition.[5]

138. It should be noted that face matching services are not designed to be used as the sole basis for ascertaining an individual's identity for evidentiary purposes. Matching results need to be corroborated by other available information about the person's identity.

139. The Participation Agreement and the NDLFRS Hosting Agreement to be established pursuant to the IGA will set out these arrangements to assist persons who may be the subject of incorrect matching results. The Department will make information available on a public website to assist individuals to raise these issues with the appropriate authorities.

140. Further information about reporting on accuracy issues is provided in the Department's response to the Committee's question on notice IMS/012 made on 17 August 2018 (available in the Department's submission 12.3 to the 2018 inquiry).

Rule-making powers in the Bill

141. In the Department's submission to the Committee of April 2018 (at paras 31-33), the Department noted the Government's intention to introduce amendments to the Bill relating to the rule-making powers. These proposed amendments were in response to comments made by the Senate Standing Committee for the Scrutiny of Bills in its *Scrutiny Digest No. 2 of 2018* tabled on 14 February 2018.

142. The Department understands that it remains the intention of the Government to continue to pursue these amendments, subject to any recommendations made by the Committee.

143. As currently drafted, the 2019 Bill contains a number of rule-making powers. These powers allow the Minister to make rules which:

- prescribe additional types of identification information (paragraph 5(1)(n))
- prescribe additional identity-matching services (paragraph 7(1)(f)), and
- prescribe additional State and Territory authorities which can access the FIS (paragraph 8(2)(q)), but only where the Minister is satisfied that the authority has law enforcement related functions of a State or Territory that previously had access to the FIS (subclause 8(3)).

144. The Minister cannot prescribe a local government agency under paragraph 8(2)(q) to have access to the FIS, as local government agencies are not agencies that have previously had law enforcement functions referred to in the Bill.

145. Rules for the purpose of paragraphs 5(1)(n), 7(1)(f) and 8(2)(q) of the 2019 Bill will be made by the Minister under clause 30 (see paragraph 30(1)(a) in particular). The Minister may also

[5] P. Jonathon Phillips et al, Proceedings of the National Academy of Sciences, *Face recognition accuracy of forensic examiners, super recognizers, and face recognition algorithms*, PNAS, 12 June 2018, 115 (24) 6171-6176, May 29, 2018, https://doi.org/10.1073/pnas.1721355115.

make rules necessary or convenient to be prescribed for carrying out or given effect to the Bill (paragraph 30(1)(b)). In making any such rules, the Minister is expressly prohibited from:

- creating criminal offences or civil penalties
- providing powers of arrest or related law enforcement functions
- imposing a tax
- appropriations, and
- direct amendment of the text of the Act.

Amendments relating to rule-making powers

146. The proposed amendments to the Bill (as mentioned above) would further strengthen safeguards relating to the Bill's rule-making powers by:

- requiring the Minister to have regard to submissions made by the Human Rights Commissioner and the Information Commissioner when making rules to prescribe additional types of identification information or new identity-matching services,
- requiring the Minister to provide reasons explaining why the rules depart from that advice (if they do), and
- providing for annual reporting in relation to the number of instances in which an entrusted person discloses protected information to lessen or prevent a threat to life or health (under clause 23).

Concluding remarks

147. The Department supports the need for robust privacy, transparency and accountability safeguards in relation to the development, operation and maintenance of the identity-matching services. The Bill does not provide broad authorisation for the use of the services by participating agencies and entities using the identity-matching services, ensuring that information sharing through the services will continue to be subject to existing privacy safeguards (including APPs and the Privacy Act) as well as other legislation.

148. The Bill contains a range of additional safeguards to protect against misuse of the information collected by the Department in the course of providing the services. These are supported by a further layer of protections established under the IGA, including the administrative and policy arrangements that support the operation of the services. These protections also operate in the context of agencies' existing oversight arrangements.

149. The Department remains open to considering suggestions from the Committee for ways in which the Bill might be improved to help ensure the responsible provision and use of the identity-matching services which are a critical component of efforts to protect Australians from identity crime and improve the delivery of government services.